INFORMATION SECURITY CONTROL AUDIT (PART II)
EXECUTIVE SUMMARY

Alarm On…Windows Locked… But The Front Door Is Open

AUDIT HIGHLIGHTS

Franchise Tax Board's (FTB) Business Entities Tax System (BETS) is the accounting system for business entity returns and related data. Authorized Designees (managers/supervisors) grants access to BETS for an employee based on their business need, workload, and job duties. The Computing Resources Bureau, Enterprise Technology Management Bureau, and Tax Systems and Application Bureau within the Technology Services Division are responsible to some degree for maintaining security controls against unauthorized access and use of taxpayer information.

Our review of access controls pertaining to BETS revealed the following major areas of concern. For more detailed information, please refer to the audit report.

- Inappropriate system access.
- System access files are not safeguarded.
- BETS access documentation is not maintained.

We acknowledge the efforts of the Technology Services Division in protecting our FTB systems from misuse. However, access controls to safeguard BETS remain weak and inadequate. These weak security controls affect our ability to protect taxpayer information to our fullest potential.

AUDITEE RESPONSE

The Computing Resources Bureau, Enterprise Technology Management Bureau, and the Tax Systems and Application Bureau within the Technology Services Division, concurred with our recommendations and provided a response for their resolutions. Please refer to Auditee Response of this report.

Exhibit 1

State of California
Franchise Tax Board

04.29.08

To: Philip Yu

From: Aleece Marendt

Internal Audit's findings for the Information Security Control Audit – Part 2

Memorandum

This memo addresses Enterprise Technology Management Bureau (ETMB) response to Internal Audit's findings for the Information Security Control Audit – Part 2. Each finding is listed below with ETMB's response in italics.

F-1 Enterprise Technology Management Bureau should:

- Reengineer the current process to secure and restrict all (FTB 8425/8427) files to authorized personnel.

The request to reengineer this process will be submitted to the IWAS web application area, Earl Bennett, manager of ETMB's Access Management Unit, spoke with Spencer Forslund, manager of IWAS group, about the request Spencer stated that because of heavy workloads he couldn't commit to when this project will start. Internal Audit should followed up on this request in July 2008

F-2 Authorized Designees should include the job related description or reason in the (FTB 8425) requests to ensure dataset access is consistent with an employee's job function.

Mainframe Security should:

- Send a reminder to Authorized Designee to include a job related description or reason in its justification for each (FTB 8425) request.
- Deny any (FTB8425) request if justification does not include job related description or are not consistent with the employee's job duties and responsibilities.

Mainframe Security will work with the ETMB's Communicate-IT staff to educate Authorized Designees about including a job related description or reason with each (FTB 8425) request. Mainframe Security will complete the education outreach by June 2008. Mainframe Security will change their procedures to include the need for a "job related description or reason" in our justification and will deny any request that does not include this. This will be completed by July 2008. It is my recommendation that Mainframe Security Staff is responsible for ensuring that the job related justification is attached. However the authorized designee should be the one responsible for ensuring that the request for access is appropriate for the employee duties.

Enterprise Technology Management
PO Box 1468
Sacramento CA 95812-3388

tel 916.845.4246
fax 916.845.4248
ftb.ca.gov

F-3 Authorized Designees should:

- Complete a (FTB 8427) request and check the "No longer in this Unit" box when an employee transfers to another unit to ensure staff access is properly remove.

Mainframe Security should:

- Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.
- Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).
- Implement an annual review of system accesses.

Mainframe Security will work with the Communicate-IT staff to educate Authorized Designee's about the proper use of the "No longer in this Unit" box this will be completed in June 2008.

Mainframe Security will work with Personnel to include the completion of the (FTB 8427) request in the personnel action form (FTB7855).

Mainframe Security will work with personnel to obtain copies of the (FTB7855) for the period of six months to perform an AS-IS evaluation of (FTB 8427) requests. Earl Bennett Manager of the Access Management unit will create a process to ensure that FTB7855 are used update employees security rights. This will be completed by October 2008.

We believe these actions will strengthen FTB's FTB 8425 and FTB 8427 processes.

Aleece Marendt, director
Enterprise Technology Management Bureau

State of California
Franchise Tax Board

05.06.08

To: Philip Yu

From: Carol Meraji

Internal Audit's findings for the Information Security Control Audit – Part 2

Memorandum

This memo addresses Computing Resources Bureau (CRB) response to Internal Audit's findings for the Information Security Control Audit – Part 2. Each finding is listed below with CRB's response in italics.

F-1 Computing Resources Bureau should:

- Remove the server address from the FTBNET2 Computer/Internet/Dataset Access Request Page.

The server administrators will review the work necessary to provide for the removal as requested; however, application modification may be necessary to achieve the desired goal. To fully achieve this, this effort should be incorporated into the reengineering of the current process, as defined by ETMB.

- Ensure logs are activated for all the 8425/8427 files to establish an audit trail for any additions, modifications, or deletions.

CRB will review the auditing capabilities on the server(s) that house the 8425/8427 processes and enable the audits, as possible, to provide adequate server auditing.

Mainframe Security should:

- Send a reminder to Authorized Designee to include a job related description or reason in its justification for each (FTB 8425) request.
- Deny any (FTB8425) request if justification does not include job related description or are not consistent with the employee's job duties and responsibilities.

CRB will assist in ETMB's effort to educate the 8425/8427 customers.

Computer Resources Bureau
PO Box 1468
Sacramento CA 95812-3388

tel 916.845.4246
fax 916.845.4246
ftb.ca.gov

F-3 Authorized Designees should:

- Complete a (FTB 8427) request and check the "No longer in this Unit" box when an employee transfers to another unit to ensure staff access is properly remove.

Mainframe Security should:

- Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.
- Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).
- Implement an annual review of system accesses.

CRB will provide support, as necessary, to ETMB to ensure that necessary actions are addressed and audit criteria are satisfied in a timely manner.

We believe these actions will strengthen FTB's FTB 8425 and FTB 8427 processes.

Carol Meraji, director
Computing Resources Bureau

STATE OF CALIFORNIA
FRANCHISE TAX BOARD
PO Box 1468
Sacramento CA 95812-3388
Telephone (916) 845-6252 Fax (916) 845-6252

M E M O R A N D U M

To: Philip Yu July 15, 2008

From: John Sulenta

Subject: Internal Audit's findings for the Information Security Control Audit – Part 2

This memo addresses Operations Management Bureau (OMB) formally known as ETMB; 60 day follow up to Internal Audit's findings for the Information Security Control Audit – Part 2. Each finding is listed below with OMB's response in italics any updates are noted in red.

F-1 Enterprise Technology Management Bureau should:

- Reengineer the current process to secure and restrict all (FTB 8425/8427) files to authorized personnel.

The request to reengineer this process will be submitted to the IWAS web application area, Earl Bennett, manager of ETMB's Access Management Unit, spoke with Spencer Forslund, manager of IWAS group, about the request Spencer stated that because of heavy workloads he couldn't commit to when this project will start. Internal Audit should followed up on this request in July 2008.

July 2008 Update: This request was submitted to the IWAS application area (end of May). We are waiting for them to schedule a meeting to discuss requirements.

F-2 Authorized Designees should include the job related description or reason in the (FTB 8425) requests to ensure dataset access is consistent with an employee's job function.

Mainframe Security should:

- Send a reminder to Authorized Designee to include a job related description or reason in its justification for each (FTB 8425) request.
- Deny any (FTB8425) request if justification does not include job related description or are not consistent with the employee's job duties and responsibilities.

Mainframe Security will work with the OMB's Communicate-IT staff to educate Authorized Designees about including a job related description or reason with each (FTB 8425)request. Mainframe Security will complete the education outreach by July 2008. Mainframe Security will change their procedures to include the need for a "job related description or reason" in our justification and will deny any request that does not include this. This will be completed by July 2008. It is my recommendation that Mainframe Security Staff is responsible for ensuring that the job related justification is attached. However the authorized designee should be the one responsible for ensuring that the request for access is appropriate for the employee duties.

July 2008 Update: Mainframe Security's procedures have been updated to request justification and a job-related description. The education and outreach effort will occur in late July or early August.

F-3 Authorized Designees should:

- Complete a (FTB 8427) request and check the "No longer in this Unit" box when an employee transfers to another unit to ensure staff access is properly remove.

Mainframe Security should:

- Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.
- Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).
- Implement an annual review of system accesses.

Mainframe Security will work with the Communicate-IT staff to educate Authorized Designee's about the proper use of the "No longer in this Unit" box this will be completed in June 2008.

July 2008 Update: Education and outreach will occur in late July or early August.

Mainframe Security will work with Personnel to include the completion of the (FTB 8427) request in the personnel action form (FTB7855).

July 2008 Update: We have met with Personnel and requested the (FTB7855) report. We will receive the report by the week of 07/22/08.

Mainframe Security will work with personnel to obtain copies of the (FTB7855) for the period of six months to perform an AS-IS evaluation of (FTB 8427) requests. Earl Bennett Manager of the Access Management unit will create a process to ensure that FTB7855 are used update employees security rights. This will be completed by October 2008.

July 2008 Update: We are waiting for the 7855 report from Personnel which we will compare to the FTB8427 requests and complete the AS IS analysis. We have discussed with Personnel about using the FTB7855's to remove rights when an employee transfers. Mainframe security will meet next week with Information Security Office Unit (ISOU) to address any issues or concerns. If there are no concerns Mainframe Security will change its procedures to include the FTB7855 form into our process.

We believe these actions will strengthen FTB's FTB 8425 and FTB 8427 processes.

John Sulenta, Service Desk Manager
Operations Management Bureau

State of California
Franchise Tax Board

04.30.2008

To: Phillip Yu, Director, Internal Audit Bureau

From: Vic Kotowski, Director, Tax Systems and Applications Bureau (TSAB)

TSAB Response to Internal Audit Findings for Information Security Control Audit – Part 2

Memorandum

The following response addresses findings F-4 and F-5 of the Information Security Control Audit – Part 2 (dated 04.17.2008).

Finding 4 (F-4): Excess mainframe system (BETS-Business Entities Tax System) accesses were granted to staff.

Internal Audit Recommendation: BETS Data Custodian should:

- Develop and execute a plan to meet with the specific areas/groups to tailor the conversations within the BE profiles for their business needs.
- Educate and train the Authorized Designees on the appropriate accesses for their business area.

TSAB Response:

1. Staff from the BETS Customer Service Team will establish recurring meetings with select business managers to review and evaluate their unique BETS user profiles. These unique 'restricted' profiles provide access to BETS for a specific business need such as Investigations, Fiscal Accounting and Fiscal Control, among others. BETS staff will work with Enterprise Technology Management Bureau (ETMB) access control personnel, as needed, to update user profiles.
2. The administration of the Authorized Designees is part of the Computing Resources Bureau (CRB) managed FTB 8427/FTB 8425 access request process and is outside of TSAB's span of control. To help educate the Authorized Designees as to the appropriate accesses for their business area, staff from the BETS Customer Service Team will provide BETS access related information to the Bureau Directors and section management for distribution to their Authorized Designees. The BETS Monthly Change Control meeting along with the BETS-INFO mail-ID/FTBNet2 Announcement will be used to communicate with the general BETS user community. In addition, the BETS Authorization Profiles web page on FTBNet2 will be updated with improved descriptions for the BETS profiles to assist business managers and Authorized Designees with preparing their FTB 8427s.
3. The BETS Customer Service Team and management are currently reviewing and updating existing internal procedures for BETS access so that support contacts with business managers and/or authorized designees will be consistent.

Tax Systems and Applications Bureau MS L270
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.6350
fax 916.845.3434
Vic.Kotowski@ftb.ca.gov

Finding 5 (F-5): The BETS Data Custodian has not updated the conversations within the BE profiles for the specified business areas/groups since inception.

Internal Audit Recommendation: BETS Data Custodian should:

- Develop and execute a plan to annually meet with the specific areas/groups to determine if any conversations within the BE profiles need to be added, modified or deleted.
- Communicate and coordinate with Mainframe Security to ensure appropriate access is given to specific areas/groups.
- Inform Authorized Designees of any new revisions to the BETS Authorizations Profiles List.

TSAB Response:

1. Staff from the BETS Customer Service Team will establish recurring annual meetings with select business managers to perform a comprehensive review and evaluation of their unique BETS user profiles. These unique 'restricted' profiles provide access to BETS for a specific business need such as Investigations, Fiscal Accounting and Fiscal Control, among others.
2. BETS staff will work with Enterprise Technology Management Bureau (ETMB) access control personnel on an annual basis and as required to keep user profiles updated.
3. Staff from the BETS Customer Service Team will meet with new external customers, when appropriate, to establish their BETS access requirements. Unique profiles are currently established for external customers to allow their BETS access to be tailored to their business need.
4. The administration of the Authorized Designees is part of the Computing Resources Bureau (CRB) managed FTB 8427/FTB 8425 access request process and is outside of TSAB's span of control. To help communicate changes or revisions to the BETS Authorizations Profiles List, staff from the BETS Customer Service Team will provide BETS access related information to the Bureau Directors and section management for distribution to their Authorized Designees. The BETS Monthly Change Control meeting along with the BETS-INFO mail-ID/FTBNet2 Announcement will be used to communicate with the general BETS user community. In addition, the BETS Authorization Profiles web page on FTBNet2 will be updated as necessary when changes or revisions are made to BETS profiles to assist business managers and Authorized Designees with preparing their FTB 8427s.

//signed//

Vic Kotowski, Director, Tax Systems and Applications Bureau

Here is the 60-day status for our responses:

F-1 Computing Resources Bureau should:

- Remove the server address from the FTBNET2 Computer/Internet/Dataset Access Request Page.

The server administrators will review the work necessary to provide for the removal as requested; however, application modification may be necessary to achieve the desired goal. To fully achieve this, this effort should be incorporated into the reengineering of the current process, as defined by ETMB.

As stated, to fully achieve this will require reengineering of the current process. In the next week, we will implement an "alias" which will hide the server name from trivial detection. The web page itself will have to be updated by the owner, which resides outside of CRB (now ISB).

- Ensure logs are activated for all the 8425/8427 files to establish an audit trail for any additions, modifications, or deletions.

CRB will review the auditing capabilities on the server(s) that house the 8425/8427 processes and enable the audits, as possible, to provide adequate server auditing.

The file auditing has been implemented on the server in question.

Six-Month Response to Internal Audit's Findings for the Information Security Control Audit – Part 2
December 15, 2008.

#	Recommendation	Six-Month Update
F-1	ETMB Should: • Re-engineer the current process to secure and restrict all (FTB8425/8427) files to authorized personnel.	Due to resource constraints, this effort has not begun. The Operations Management Bureau's (OMB) Access Management Unit assumed second-level Mainframe Security responsibility in October of 2008. As part of the transfer of responsibility, the Access Management unit received an additional position for second-level Mainframe Security support. The position will be filled in late December. We anticipate beginning the process evaluation effort in February of 2009 and the effort taking approximately three months.
	CRB should: • Remove the server address from the FTBNet2 Computer/Internet/Dataset Access Request Page	Completed by Server Management Section (SMS), Internal Web and Admin Systems (IWAS) Bureau, and OMB staff December 2008. Additionally, all other references to this address (i.e. Google Search results) were updated in accordance with the internal audit recommendation. This effort was coordinated and completed by IWAS staff December 2008.
	CRB should: • Ensure logs are activated for all the (FTB8425/8427) files to establish an audit trail for any additions, modifications, or deletions.	Completed by SMS staff in August 2008.
F-2	Authorized Designees should include the job related description or reason in the (FTB8425) requests to ensure dataset access is consistent with an employee's job function. Mainframe Security should: • Send a reminder to Authorized Designees to include a job related description or reason in its justification for each (FTB 8425) request.	OMB's Access Management Unit coordinated an announcement through Communicate IT reminding authorized designees to include job related justification with each FTB8425. Communicate IT sent the announcement in August 2008.
	Mainframe Security should: • Deny any (FTB 8425) request if justifications do not include job related description or are not consistent with the employee's job duties or responsibilities.	OMB's Access Management Unit implemented this process in August 2008.
F-3	Authorized Designee should: • Complete a (FTB8427) request and check the "No Longer in this Unit" box when an employee transfers to another unit to ensure staff system access is properly removed.	OMB's Access Management Unit coordinated an announcement through Communicate IT reminding authorized designees to check the "No Longer In This Unit" box when an employee transfers to another unit. Communicate IT sent the announcement in August 2008.
	Mainframe Security should: • Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.	Personnel provided OMB's Access Management Unit all 7855 forms completed between May 2008 and October 2008. Access Management staff will perform a random sample and report findings to the manager of the IT Service Desk section by the end of January 2009.
	• Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).	OMB's Access Management Unit staff will work with Personnel to implement a new process by May 2009.
	• Implement an annual review of system accesses.	OMB's Access Management Unit staff developed procedures and will begin annual process in January 2009. The process will take approximately two months.

State of California
Franchise Tax Board

November 7, 2008

To: Dina Felisilda

From: Catherine Dai, Manager of BETS Systems and Testing Support Unit

6 Month Follow-Up - Information Security Control Audit (Part II)

Memorandum

The purpose of this memo is to provide Internal Audit the 6 month update of our efforts to implement the recommendations provided to us. As previously reported, an audit was performed by FTB Internal Audit on May of 2008. The audit identified some Business Entities Tax System (BETS) security access controls issues. Based on the results of the audit, Internal Audit staff suggested BETS staff to work with the BETS users closely in order to make sure the appropriate BETS security access is given based on business needs. In addition, Internal Audit staff also suggested BETS staff to work with the business areas to ensure the existing BE security profiles (BEPRO) are meeting their business needs. If necessary, BE security profiles should be added, modified or deleted as appropriate to align with the business needs.

As soon as BETS managers received the audit's results and suggestions, the following actions have been or will be taken:

- In July 2008, the manager of Tax Systems and Applications Bureau (TSAB) Testing Section provided a memo (see attached) to FTB Managers and Supervisors to explain the situation and ask the business managers to review the BETS access (BEPRO) listed on the FTB 8427 of their staff. Accompanied with the memo, BETS Conversations descriptions and BETS BEPRO definitions were provided for references.
- In addition to the memo mentioned above, the BETS Customer Services staff had brought this item up in the monthly BE Change Control Meeting to discuss with the users in order to answer any questions that they may have.
- Since the memo was sent out, multiple business areas had contacted BETS Customer Services staff to inquire and correct the BETS profiles for their staff. Below are some of the contacts received by BETS Customer Services staff:

TSAB Tax Systems Testing Section MS L-210
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.6229
fax 916.845.3434
Catherine.dai@ftb.ca.gov

  - District Office (Houston and Sacramento) asked to remove BEPRO** (this profile allows users to perform the main BETS transactions) from their collectors and auditors since they just need view only access. They have a support unit that performs their BETS transactions.
  - Investigations Unit – They made revisions to their BEPRO's that staff have access to.
  - Collections Unit - They removed BEPRO*** from their staff access since they do not perform BETS transactions.
  - IVR Unit – They also removed BEPRO** and only need view access.
  - Service Transition Section – They reviewed their BETS accesses and revised their staff's FTB 8427 based on their business needs.
  - BES staff is constantly reviewing their BETS BEPRO accesses. They called with some general questions. They are currently reviewing BETS Code Table Accesses as well.
- In the area of BETS Access education, BETS Customer Services Team is in the process of reviewing and revising the information on the FTBNET for BETS BEPRO's and Conversations. This action is triggered by the feedback that was provided by the business areas. Some of the business users commented about the difficulties they have had trying to understand the BETS accesses and BETS BEPROS information posted on the FTBNET. The plan is to have the information updated by February of 2009.
- Another action that the BETS Customer Services Team will be taken to address the access issue is to continue working with the business areas on customizing some of the BEPROs in order to meet their specific business needs.
- The BETS Customer Services Manager plans to follow up with the business areas in January of 2009 to remind and assist review of the FTB 8427 for BETS accesses. This process will be an annual process scheduled on January of each year.

The BETS Customer Services Team strives for providing the best customer services to the departmental users and following the FTB security access guidelines. We appreciate any comments or suggestions that can help us to improve our services.

NOTE: ((***)) = Indicates confidential and/or proprietary information has been redacted (Government Code section 6254.9).

Thank you,

Catherine Dai
Manager, BETS Systems and Testing Support Unit
Ph#: 845-6229

Philip Yu
Andrea VanWalleghem.
Vic Kotowski
Carol Meraji
John Sulenta
Wendy Naismith
Roy Couch

Twelve-Month Response to Internal Audit's Findings for the Information Security Control Audit – Part 2 **May 28, 2009**

#	Recommendation	Six-Month Update
F-1	ETMB Should: • Re-engineer the current process to secure and restrict all (FTB8425/8427) files to authorized personnel.	Due to resource constraints, this effort has not begun. The Operations Management Bureau's (OMB) Access Management Unit assumed second-level Mainframe Security responsibility in October of 2008. As part of the transfer of responsibility, the Access Management unit received an additional position for second-level Mainframe Security support. The position will be filled in late December. We anticipate beginning the process evaluation effort in February of 2009 and the effort taking approximately three months. **May 2009 Update** - The evaluation began in May 2009, but because of resource constraints will take four month to complete.
	CRB should: • Remove the server address from the FTBNet2 Computer/Internet/Dataset Access Request Page	Completed by Server Management Section (SMS**),** Internal Web and Admin Systems (IWAS) Bureau, and OMB staff December 2008. Additionally, all other references to this address (i.e. Google Search results) were updated in accordance with the internal audit recommendation. This effort was coordinated and completed by IWAS staff December 2008.
	CRB should: • Ensure logs are activated for all the (FTB8425/8427) files to establish an audit trail for any additions, modifications, or deletions.	Completed by SMS staff in August 2008.
F-2	Authorized Designees should include the job related description or reason in the (FTB8425) requests to ensure dataset access is consistent with an employee's job function. Mainframe Security should: • Send a reminder to Authorized Designees to include a job related description or reason in its justification for each (FTB 8425) request.	OMB's Access Management Unit coordinated an announcement through Communicate IT reminding authorized designees to include job related justification with each FTB8425. Communicate IT sent the announcement in August 2008.
	Mainframe Security should: • Deny any (FTB 8425) request if justifications do not include job related description or are not consistent with the employee's job duties or responsibilities.	OMB's Access Management Unit implemented this process in August 2008.
F-3	Authorized Designee should: • Complete a (FTB8427) request and check the "No Longer in this Unit" box when an employee transfers to another unit to ensure staff system access is properly removed.	OMB's Access Management Unit coordinated an announcement through Communicate IT reminding authorized designees to check the "No Longer In This Unit" box when an employee transfers to another unit. Communicate IT sent the announcement in August 2008.
	Mainframe Security should: • Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.	Personnel provided OMB's Access Management Unit all 7855 forms completed between April 2008 and September 2008. Access Management staff will perform a random sample and report findings to the manager of the IT Service Desk section by the end of January 2009. **May 2009 Update** – For the April through September 2008 7855 forms, there were 592 users that transferred from one unit within FTB t another or moved to a new agency. During the same period, there were 34 accounts that had a matching 8427. Based on the number o matches (34) vs the number of 7855's (592), it appears supervisors and managers submitted 8427 forms only 6% of the time when a employee left their unit.
	• Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).	**May 2009 Update** - OMB's Access Management Unit staff will work with Personnel to implement a new internal process by June 2009.
	• Implement an annual review of system accesses.	OMB's Access Management Unit staff developed procedures and will begin annual process in January 2009. **May 2009 Update** - The process is 60% complete. Estimated completion date August 2009.

State of California
Franchise Tax Board

May 8th, 2009

To: Dina Felisilda
From: Cathrine Dai

Subject: 6 month follow up – Information Security Control Audit

Memorandum

In a prior memo addressed to Dina Felisilda, dated November 7, 2008, the Business Entities Tax System (BETS) committed to Internal Audit to provide 6 month updates of our efforts to implement the recommendations made as a result of the Information Security Control Audit that was performed in May 2008. In the memo referenced above, BETS was to perform certain follow up actions.

The overall focus for BETS was to work closely with our customers to assist, educate, streamline, and enhance processes surrounding BE Security Profiles (BEPRO). In order to accomplish the desired goal, communication with our customers has been increased so that user needs can be clearly defined. In doing so, BETS has still been able to provide the appropriate services while insuring that security access is given in a timely fashion based on the customer's specific business needs. The following actions have taken place and/or are currently ongoing to accomplish our goal:

- In an effort to reach out to our customers, BETS Customer Services has created an open line of communication with Supervisors and Managers directly responsible for making changes to user BEPROs. As a result, our customer has become better educated on all BEPROs, therefore reducing the amount of confusion surrounding the current BEPRO structures.
- As an ongoing effort, BETS Customer Services continues to compile information so that BEPROs can be customized to meet the business needs of the customer.
- BETS Customer Services has continued to utilize the BE user representative and BE Change Control Meetings as platforms to address questions and /or concerns regarding BEPROs. This has also been a useful way to communicate with the customer.
- As of the current date, BETS Customer Services is still exploring the possibility of revising the current FTB NET web page so that it can be a useful tool to our customer. This is directly associated with the revision or customization of existing BEPROs.

Section or Division MS 0000
PO Box 0000
Sacramento CA 95800-0000

tel 916.845.0000
fax 916.845.0000
ftb.ca.gov

- The BETS Customer Services Manager continues to closely oversee that the appropriate actions are taking place to create a process to update and maintain BEPROs that is easily understandable and accessible to our customers. The FTB security access guidelines will continue to be reinforced so that BETS and its customers are in compliance with all applicable guidelines.
- As indicated in our last follow up, we also intend to continually work with our customer to review their FTB 8427's to ensure that they are in line with their business needs.

The BETS Customer Services Team works closely with all customers to provide exceptional customer service while maintaining the integrity of the FTB security access guidelines. Your feedback is encouraged and we appreciate any comments or suggestions that you would like to provide.

Thank You,

Catherine Dai
Manager, BETS Testing and System Support Section

CC: Phillip Yu
Andrea VanWellinghem
Vic Kotowski
Carol Meraji
John Sulenta
Wendy Naismith
Roy Couch

BETS Conversation Descriptions

***** Taxpayer Look-Up Inquiry Look up Entity Partial ID or Name.

***** Add New Taxpayer allows you to add a taxpayer.

***** Maintain ID allows you to view, add or update entity ID's.

***** Maintain Name allows you to view, add or update entity name or DBA name.

***** Maintain Business Details allows you to view, add or update entity business details.

***** Maintain Notes allow you to view, add or update entity notes.

***** Maintain Assets allow you to view, add or update entity assets.

***** Maintain Address allows you to view, add or update business addresses.

***** Maintain Relationships allows you to view, add business relationships.

***** Maintain Exemptions allows you to view, add or update taxpayer's exemptions.

***** Maintain Account allows you to view, add or update business accounts.

***** Record Returned Mail allows you to record returned mail for BETS generated notices.

***** ID Inquiry allows you to view entity ID's.

***** Name Inquiry allows you to view entity name or DBA name.

***** Business Details Inquiry allows you to view entity business details.

***** Notes Inquiry allows you to view addresses.

***** Asset Inquiry allows you to view entity assets information.

***** Address Inquiry allows you to view entities address information.

***** Relationships Inquiry allows you to view business relationships.

***** Exemptions Inquiry allows you to view taxpayer's exemptions.

***** Account Inquiry allows you to view business accounts.

***** Entity Profile Inquiry allows you an overall view of entity address, business and accounts.

***** Indicator Inquiry allows you to view non-financial indicators.

***** Organization Inquiry allows you to view organization information and reporting structures.

***** Maintain Stage Criteria allows you to set DLC criteria.

***** Maintain Organization allows you to add or update organization information. (BETS HD)

***** Maintain Employee allows you to add or update employee details.

***** Employee Inquiry allows you to view employee details.

NOTE: ((***)) = Indicates confidential and/or proprietary information has been redacted (Government Code section 6254.9).

BETS Conversation Descriptions

***** Condition Request allows you to view DLC criteria.

***** Maintain Contract allows you add or delete Water's Edge contract information.

***** Contract Inquiry allows you to view Water's Edge contract information.

***** Suspense Transaction Inquiry allows you to view the details of the return or payment and reason for the item being suspended.

***** Suspended Batch Correction allows you to recycle suspended batches.

***** Correct Suspense Transactions allows you to make changes to the return or payment.

***** Review, Refunds, Credit and Bill Request allow ALL Users to view Refunds and Bills. Allows authorized users to:

- Hold or approve refunds
- Generate a refund request without a return being filed.
- Reallocate credit to a refund request
- Hold or approve bills
- Do a manual refund

***** Suspension Transaction allows you to view a suppression or release/update the suppression.

***** Source Document Request allows you to request paper returns from DS&S.

***** Account Period Adjustments allows you to adjust taxpayer accounts, account periods or specific assessments. The following transactions are available using this.

- API Change-
- Due Date – Change the due date of the return
- Penalty – Assess penalties and/or interest
- File Period – Change the file period
- Abate – abate dynamic penalties and/or interest
- Discharge – perform and discharge on the balance due
- Write-off – write-off the balance due on the account
- Credit – Apply excess credit to another account period
- Offset –Offset credit on tax year to another tax year
- PIADDJ – An (hard) adjustment to penalties and/or interest.

***** Account Period Profile Inquiry allows you to view financial information for a BETS taxpayer

***** Deleted Transaction List allows you to locate a converted payment on BETS.

***** Transaction Adjustment allows you to make the following adjustment transactions.

- NGCheck - Add a bad check assessment with penalties
- LIADJ – Update line items
- Reverse – Places payment into suspense (R504)
- InDate – Update the in-date (eff. date of pay doc or source doc
- Revpymt – Reverse misapplied payments
- NGNPT – Add a bad check assessment with no penalties

NOTE: ((***)) = Indicates confidential and/or proprietary information has been redacted (Government Code section 6254.9).

BETS Conversation Descriptions

***** Transfer Adjustment allows the user to transfer returns to suspense, or direct transfer payments across entity ID's, account types and/or account periods.

***** Delete Account allows you to delete an account period.

***** Summary Balance Inquiry allows you to view financial information for a taxpayer.

***** Record Questionable Filer allows you to indicate a taxpayer is under investigation

***** External Liability Inquiry allows you to view offsets to BOE or EDD (pending or final).

***** Maintain External Liability allows you to add or update information regarding offsets to BOE or EDD.

***** Maintain Indicator allows you to add or modify non financial account indicators.

***** Maintain Review allows you to view a list of transactions under review.

***** Payment Application allows you to create an in-lieu to be keyed in ICBS for a payment, when Entity is known.

***** Suspense Account allows you to create an in-lieu to be keyed in ICBS for a payment, when Entity is unknown.

***** Suspense Account Research/Transfer allows you to correct and transfer payments from suspense to R208.

***** Fund Transfer Inquiry allows you to view payments that have been transferred out of BETS.

***** Payment Application Inquiry allows you to view how payments have been applied.

***** Maintain Case allows you to view, add, or modify a DLC case.

***** Case Inquiry allows you to view a DLC case.

***** Maintain Lien allows you add or modify LIEN information.

***** Lien Inquiry allows you to view LIEN information.

***** Maintain NPA allows you to create, revise or review NPA's.

***** Maintain NPA Case allows you to view NPA's and if authorized, modify the status of an NPA.

***** Notice Composition allows you to create a notice request. (Please Note: Notices are generally generated by the system.)

***** Notice Inquiry allows you to view detail of an issued or scheduled notice.

NOTE: ((***)) = Indicates confidential and/or proprietary information has been redacted (Government Code section 6254.9).

State of California
Franchise Tax Board

05.08.08

To: Carol Meraji, Director
Computing Resources Bureau

Aleece Marendt, Director
Enterprise Technology Management Bureau

Vic Kotowski, Director
Tax System & Applications Bureau

From: Philip Yu

Information Security Control Audit (Part II)

Alarm On…Windows Locked… But The Front Door Is Open

Memorandum

The Information Security Control Audit (ISCA) was developed primarily in following with the National Institute of Standards and Technology (NIST) Special Publication 800-53 and 800-53A. ISCA is divided into two parts. Part I focused on four security-related control areas (families) pertaining to the Privacy, Security and Disclosure Bureau (PSDB). Part II is focused on one security-related control area, Access Controls, as it pertains to the Business Entities Tax System (BETS) only.

This report provides a reasonable measure of existing security effectiveness[1]. As such, business managers will learn where security improvements may be made. This report may 1) partially satisfy the Federal Information Security Management Act of 2002 reporting requirements; 2) support continuing monitoring requirements; and 3) identify resource needs to improve our security program. However, this audit does not determine if FTB has selected the appropriate set of security controls to achieve adequate security in protecting taxpayer information.

AUDIT OBJECTIVE & SCOPE

The audit objective is to review access controls pertaining to BETS and provide management reasonable assurance that existing security controls are implemented and operating as intended at the system level for protection against unauthorized access and use of taxpayer information.

The scope of this audit included activities from September 2006 to present.

[1] Federal Information Processing Standards (FIPS) Publication 200 states that an organization must implement the minimum-security requirements and ensure their effective implementation.

Internal Audit Bureau MS F161
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.3388
fax 916.845.0733
ftb.ca.gov

METHODOLOGY

To achieve our audit objective, the internal audit team:

- Researched and reviewed relevant or applicable policies, regulations, industry standards and best practices (NIST Special Publication).
- Developed specific security control focused questionnaires incorporating applicable policies, regulations, and industry standards.
- In certain instances, we observed the Filing Division's processes, performed random sample testing of data to corroborate representation or information we obtained.
- Most of the data was received from four areas within the Filing Division; however, we also received information from the Security Support Unit and PSDB that support the Filing Division's control activities.

RESULTS

The following is a summary of the auditors' findings. For more detailed information of findings and recommendations, please see Appendix A.

FINDINGS

F-1	The server that stores (FTB 8425/8427) files is vulnerable to unauthorized access and manipulation.
F-2	Mainframe dataset access is granted to staff without adequate justification.
F-3	Staff transferring to another Unit within FTB retained system accesses not required for their new position.
F-4	Excess mainframe system (BETS-Business Entities Tax System) accesses were granted to staff.
F-5	The BETS Data Custodian has not updated the conversations within the BE profiles for the specified business areas/groups since inception.

RECOMMENDATIONS

F-1	Enterprise Technology Management Bureau should: • Reengineer the current process to secure and restrict all (FTB 8425/8427) files to authorized personnel. Computer Resources Bureau should: • Remove the server address from the FTBNet2 Computer/Internet/Dataset Access Request Page. • Ensure logs are activated for all the (FTB 8425/8427) files to establish an audit trail for any additions, modifications, or deletions.
F-2	Authorized Designees should include the job related description or reason in the (FTB 8425) requests to ensure dataset access is consistent with an employee's job function. Mainframe Security should: • Send a reminder to Authorized Designees to include a job related description or reason in its justification for each (FTB 8425) request. • Deny any (FTB 8425) request if justifications do not include job related description or are not consistent with the employee's job duties and responsibilities.
F-3	Authorized Designees should: • Complete a (FTB 8427) request and check the "No longer in this Unit" box when an employee transfers to another Unit to ensure staff system access is properly removed. Mainframe Security should: • Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes. • Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855). • Implement an annual review of system accesses.
F-4	BETS Data Custodian should: • Develop and execute a plan to meet with the specific areas/groups to tailor the conversations within the BE profiles for their business needs. • Educate and train the Authorized Designees on the appropriate accesses for their business area.

RECOMMENDATIONS (Continued)

F-5	BETS Data Custodian should: • Develop and execute a plan to annually meet with the specific areas/groups to determine if any conversations within the BE profiles need to be added, modified or deleted. • Communicate and coordinate with Mainframe Security to ensure appropriate access is given to specific areas/groups. • Inform Authorized Designees of any new revisions to the BETS Authorization Profiles List.

CONCLUSION

Based on our review, the security controls to safeguard the Business Entities Tax System is weak and inefficient due to the following issues: ability to access and manipulate the server that stores (FTB 8425/8427) files, mainframe datasets are granted with inadequate justification, and the most restricted set of rights/privileges are not being assigned to users based on their job duties. These inadequacies affect our ability to protect taxpayer information to our fullest potential.

Please inform Internal Audit in writing, of your efforts to implement the recommendations after 60 days, 6 months, and 1 year from the date of this final report. The information you provide us will be used to determine the need for a follow-up review.

We greatly appreciate the cooperation and assistance provided to us by your staff during our review. If you have any questions, please contact Lynnette Chan at 845-4790 or Dina Felisilda at 845-6234.

Philip Yu, Director
Internal Audit Bureau

cc: S. Stanislaus
L. Iwafuchi
C. Cleek
L. Crowe

APPENDIX A

FINDINGS & RECOMMENDATIONS

FINDING 1 (F-1): **The server that stores (FTB 8425/8427) files is vulnerable to unauthorized access and manipulation.**

CONDITION: The Dataset Access Request (FTB 8425) and the Computer Access Request (FTB8427) Internet Forms are utilized to establish, modify, or remove mainframe dataset/system accesses. When a (FTB 8425/8427) request is submitted, files on the server are queried to determine if the requestor is an authorized designee, then the data on the request updates the appropriate (FTB 8425/8427) files.

The information on the (FTB 8425/8427) files includes, but are not limited to the following:

- User –Name, User ID, Payroll Unit Code (PUC) and Production Accesses.
- Authorized Designee - Supervisors/managers authorized to submit the (FTB 8425/8427) request.
- History – Completed (FTB 8425/8427) requests.

The auditors found the (FTB 8425/8427) files are not secured and the actual address of the server is noted on the FTBNet2 Computer/Internet/Dataset Access Request Page. Any FTB employee has the capability to access the above-mentioned files without any restrictions. As a result, any FTB employee can:

- Add themselves as Authorized Designees.
- Add, modify or delete current or historical data, without leaving an audit trail.

In two instances, unauthorized access caused the (FTB 8425/8427) request process to stop working for 2 days.

CRITERIA: ISP 410 states, "Data Owners and Data Custodians of all FTB systems, with the review and approval of the FTB Chief Security Officer (CSO), must restrict those functions and processes that can be misused to compromise the security or availability of systems and data."

EFFECT: Any FTB employee can add, modify, or delete data within the (FTB 8425/8427) files without leaving an audit trail. This course of action may compromise mainframe systems or cause a disruption in the web-based (FTB 8425/8427) request process.

CAUSE: The (FTB 8425/8427) files on the server are not restricted to authorized personnel.

(FINDING 1 (F-1) CON'T)

RECOMMENDATION:

Enterprise Technology Management Bureau should:

- Reengineer the current process to secure and restrict all (FTB 8425/8427) files to authorized personnel.

Computer Resources Bureau should:

- Remove the server address from the FTBNet2 Computer/Internet/Dataset Access Request Page.
- Ensure logs are activated for all the (FTB 8425/8427) files to establish an audit trail for any additions, modifications, or deletions.

FINDING 2 (F-2): **Mainframe dataset access is granted to staff without adequate justification.**

CONDITION: Authorized Designees (supervisors/managers) utilize the Dataset Access Request Form (FTB 8425) to add, modify, or remove mainframe dataset access. Datasets are grouped by mainframe systems such as:

- Business Entities Tax System (BETS)
- Taxpayer Information System (TI)
- Accounts Receivable Collections System (ARCS)
- Professional Audit Support System (PASS)

The auditor found dataset capabilities are significant because data is used for batch processes, return information, payments and interface type transactions between Collections and BETS. Some datasets give an employee access to all data and mainframe systems.

The auditors randomly reviewed 20% of the total population (1252 records) and identified that 48% of the justifications did not provide a job related description or reason for the dataset access request. Some of the justifications used in the (FTB 8425) requests are listed below:

Access has expired	For review purposes
Access needed for maintenance purposes	George needs this
Access needed for production support	Need to read data to verify the data
Access required to perform testing	Needs access for statistical study
Build test data	New Employee

CRITERIA: GPM 7010 states, "Authorized Designees must ensure that the request for dataset access is consistent with the employee's job duties and responsibilities. In addition, Authorized Designees need to enter the necessary justification for access to the requested datasets."

EFFECT: Staff could be granted more access than required to perform their job duties and responsibilities.

CAUSE: Authorized Designees submit (FTB 8425) requests with vague/generic justifications that do not support a specific job function.

(FINDING 2 (F-2) CON'T)

RECOMMENDATION:

Authorized Designees should include the job related description or reason in the (FTB 8425) requests to ensure dataset access is consistent with an employee's job function.

Mainframe Security should:

- Send a reminder to Authorized Designees to include a job related description or reason in its justification for each (FTB 8425) request.
- Deny any (FTB 8425) request if justifications do not include job related description or are not consistent with the employee's job duties and responsibilities.

FINDING 3 (F-3): **Staff transferring to another Unit within FTB retained system accesses not required for their new position.**

CONDITION: Authorized Designees (supervisors/managers) utilize the Computer Access Request Form (FTB 8427) to establish, modify, or remove mainframe system accesses. For employee transfers within FTB, the outgoing supervisor is required to complete the (FTB 8427) request and check the "No longer in this Unit" box. The incoming supervisor must complete a (FTB 8427) request indicating the employee's new Payroll Unit Code (PUC), resources, profiles, facilities, and/or remote access methods.

In addition, Timekeepers complete a Personnel Action Form (FTB 7855) for any employment and/or position changes.

The auditors found when the outgoing supervisor did not submit the (FTB 8427) request with "No longer in this Unit", an employee retained their former system accesses. As a result, when the incoming supervisor submits the new (FTB 8427) request, Mainframe Security:

- Must complete additional transactions to reconcile the discrepancies between the new PUC (access request) and Top Secret (former system accesses).

However, when the new supervisor does not update the new PUC, employees will retain their system accesses and Mainframe Security will not know there is a discrepancy to reconcile.

CRITERIA: GPM 7010 states, "When an employee transfers to another Unit within FTB, the supervisor of the Unit from which the employee is leaving shall complete an FTB 8427 with a check in the "No longer in this Unit" box."

EFFECT:

- Staff retains system access that may be inappropriate for their new job.
- Staff may view information or perform transactions outside of their business need (in excess).

CAUSE: The outgoing supervisor forgets to complete a (FTB 8427) request with the "No longer in this Unit" box.

(FINDING 3 (F-3) CON'T)

RECOMMENDATION:

Authorized Designees should:

- Complete a (FTB 8427) request and check the "No longer in this Unit" box when an employee transfers to another Unit to ensure staff system access is properly removed.

Mainframe Security should:

- Perform a review of the current system accesses by obtaining copies of the (FTB 7855) submitted within the last 6 months to ensure a (FTB 8427) request has been submitted for all employee transfers or position changes.
- Work with Personnel to include the completion of the (FTB 8427) request in the Personnel Action Form (FTB 7855).
- Implement an annual review of system accesses.

FINDING 4 (F-4): **Excess mainframe system (BETS-Business Entities Tax System) accesses were granted to staff.**

CONDITION: Authorized Designees (supervisors/managers) grant mainframe system (BETS) accesses to their staff by requesting through the Computer Access Request (FTB 8427). Often, supervisors grant accesses by mirroring accesses held by current or past staff. Twelve of the twenty-five staff reviewed had accesses in excess of what was needed for their work. Upon notification of the excess accesses, supervisors quickly removed the excess accesses.

CRITERIA: ISP 410 states, "Data Owners and Data Custodians of all FTB systems, with the review and approval of the FTB Chief Security Officer (CSO), must restrict those functions and processes that can be misused to compromise the security or availability of systems and data."

NIST SP 800-53 Access Control Policies and Procedures states, "the organization develops, disseminates, and periodically reviews/updates formal documented procedures to facilitate the implementation of the access control policy and associated access controls."

EFFECT: Employees are able to perform transactions in excess of their business need.

CAUSE:

- Supervisors have difficulty choosing a profile for their staff. There are dozens of BE profiles and each profile may include a dozen conversations (transactions).
- The BE profiles and their conversations were created 10 years ago. These BE profiles (as they are) may not be appropriate for these business areas and often provide accesses (conversations) that are in excess of their business need.

RECOMMENDATION:

BETS Data Custodian should:

- Develop and execute a plan to meet with the specific areas/groups to tailor the conversations within the BE profiles for their business needs.
- Educate and train the Authorized Designees on the appropriate accesses for their business area.

FINDING 5 (F-5): **The BETS Data Custodian has not updated the conversations within the BE profiles for the specified business areas/groups since inception.**

CONDITION: The BETS Authorization Profiles Listing contains BE profiles that have been established for BETS users and/or specific groups. Each BE profile includes a set of conversations that allow a user to view or perform transactions in BETS. The BETS Data Custodian is responsible for updating the BETS Authorization Profiles Listing.

The BETS Authorization Profiles Listing is utilized by:

- Authorized Designees (supervisors/managers) to add/update an employee's BETS accesses.
- Mainframe Security to determine whether access should be granted.

The auditor found some specified business areas/groups were given inappropriate system accesses. For example, BE profile ** is set for Investigations staff and contains 7 conversations (****, ****, ****, etc.); though Investigations staff may only need 3 of 7 conversations, all 7 conversations are granted.

CRITERIA: ISP 410 states, "Data Owners and Data Custodians of all FTB systems, with the review and approval of the FTB Chief Security Officer (CSO), must restrict those functions and processes that can be misused to compromise the security or availability of systems and data."

NIST SP 800-53 Access Control Policies and Procedures states, "the organization develops, disseminates, and periodically reviews/updates formal documented procedures to facilitate the implementation of the access control policy and associated access controls."

EFFECT:

- Authorized Designees do not have an accurate BE profile listing to determine appropriate accesses for staff.
- Mainframe Security may grant inappropriate accesses.
- Staff may have system accesses that may not be within their "need to know" or job function.

CAUSE:

- The BETS Authorization Profiles List was not maintained on a regular basis.
- Due to workload priorities, the BETS Data Custodian has not met with the designated business areas/groups to ensure the BETS conversations are still appropriate for their job functions.

(FINDING 5 (F-5) CON'T)

RECOMMENDATION:

BETS Data Custodian should:

- Develop and execute a plan to annually meet with the specific areas/groups to determine if any conversations within the BE profiles need to be added, modified or deleted.
- Communicate and coordinate with Mainframe Security to ensure appropriate access is given to specific areas/groups.
- Inform Authorized Designees of any new revisions to the BETS Authorization Profiles List.

APPENDIX B

RESPONSES TO RECOMMENDATIONS

Internal Audit Bureau MS F161
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.3388
fax 916.845.0733
ftb.ca.gov

APPENDIX C

EVALUATION OF RESPONSES